CHAPTER 1
ADDENDUM B

NIPRNET PORTS AND PROTOCOLS SECURITY TECHNICAL GUIDANCE

DEPARTMENT OF DEFENSE
NIPRNET PORTS & PROTOCOLS SECURITY TECHNICAL GUIDANCE
FEBRUARY 2002

1 REFERENCES

1.1 DoD CIO Guidance and Policy Memorandum 6-8510- Department of Defense Global Information Grid Information Assurance and Information Assurance Implementation Guidance, June 16, 2000

1.2 CJCSI 6510.01C, May01, DoD Information Assurance Implementation Guidance And Policy Memorandum, Subject: Department Of Defense Interim NIPRNET Ports & Protocols Technical Guidance - January 2002

1.3 Chairman of the Joint Chiefs Staff Instruction (CJCSI) 6510.01C, 1 August 2000 Final Draft, "Information Assurance (IA) and Computer Network Defense (CND)

1.4 Department of Defense Chief Information Officer Guidance and Policy Memorandum No. 6-8510 "Department of Defense Global Information Grid Information Assurance"

1.5 The Internet Assigned Numbers Authority, Protocol Numbers and Assignment Services, http://www.iana.org/

1.6 Internet Engineering Task Force (IETF) RFC 0792, Internet Control Message Protocol, September 1981, http://www.ietf.org/rfc/rfc0792.txt?number=792

2 PURPOSE

In keeping with the principles of defense in depth required by references 1.1 and 1.2, this document establishes interim technical guidance on detailed configuration settings for known, identified combinations of ports, protocols, and services (PPS) for perimeter defense (firewalls, etc.) implementations for networks connected to the NIPRNET, and for networks connected to the NIPRNET while simultaneously having an approved connection(s) directly to the Internet. The detailed technical guidance on specific PPS is found in the tables in Section 0 of this document. It is also available at http://www.cert.smil.mil. These tables provide detailed configuration settings for known, identified combinations of ports, protocols, and services (PPS). The guidance includes recommended security countermeasures for minimizing the vulnerabilities for use of risky PPS that are used by

essential applications. This technical security guidance provides the basis for evaluating the level of technical risk and recommended mitigation of the various PPS.

3 BACKGROUND

This guidance responds to a network management need identified by the Information Assurance Panel (IAP) of the Military Communications-Electronics Board (MCEB). This interim guidance provides for all users of the NIPRNET, including DoD, other government agencies (for example USCG, FAA), and selected commercial contractors, while waiting final staffing and publication of appropriate directives in the 8500 and 6500 series. The guidance supports several goals:

- To ensure interoperability across NIPRNET for all users, e.g. DoD CINCs/Services/Agencies (C/S/As);
- To mitigate common risk within the NIPRNET user community;
- To create a common development environment by providing security guidance to system developers.

The understanding of mutually accepted risk within the NIPRNET seeks to provide maximum interoperability with an emphasis on security. The logic is that all participants inside the NIPRNET share a common level of risk to their systems, defined by the protections established at the NIPRNET/Internet boundary, and the minimum level of protection found at all internal enclave boundaries to the NIPRNET backbone. An enclave is any network under the operational control and authority of a single organization with the responsibility to define and implement security controls. The guidance includes DoD community requirements for perimeter defense implementations with detailed configuration settings for PPS and recommended security countermeasures for minimizing the vulnerabilities for use of risky PPS that have an inter-C/S/A operational requirement. A description of the evaluation process is included as Attachment A.

4 SCOPE

This guidance applies to all DoD Components and government network security devices serving as network boundaries to the NIPRNET, to include in garrison and deployed implementations. It also applies to security boundaries of networks with approved connections directly to the Internet. The scope of this document is to provide common configurations for PPS used to communicate with other users on the NIPRNet.

4.1 PROTOCOLS ADDRESSED

This guidance is limited to protocols that correspond to the Internet Protocol (IP) Suite as described by IANA. This interim guidance only covers the three most widely used and needed protocols: Internet Control Messaging Protocol (ICMP) (protocol 1), Transmission Control Protocol (TCP) (protocol 6) and User Datagram Protocol (UDP) (protocol 17).

4.2 VIRTUAL PRIVATE NETWORKS

A Virtual Private Network is an encrypted tunnel that can transport Internet protocols securely between enclaves depending on policy. This document does not extend to DoD/

government service or agency internal network boundaries or their use of Virtual Private Networks (VPN). Within such enclave networks and enclaves extended via VPN, the use of ports and protocols services will be governed by internal organizational policy. Authorities operating VPNs are responsible for security controls over data content traversing their VPN connections.

Additionally, VPN are used to securely extend enclaves and to link organizations. When an organization uses a VPN to bypass other security processes (e.g. firewall, intrusion detection systems) they potentially introduce new vulnerabilities to the network. The assumption is that the lowest common security policy will apply unless the VPN is subjected to firewall rules. Hence, it is recommended that VPN traffic still be subject to firewall rules because of the possibility of differing security policies and postures between organizations.

Security managers may consider allowing use of selected PPS listed as ***Red*** (high risk) between enclaves of a given NIPRNet user through a VPN connection. This technique would hide the PPS from implemented perimeter defense security solutions and allow traffic that is not nominally conforming to this guidance. However, it is essential to keep in mind that such action could expose either enclave involved in the VPN to added risks from the other. Should this happen, the newly exposed enclave could in turn endanger other enclaves on the NIPRNET using allowed connection external to the VPN. Therefore, this analysis for each case to allow ***Red*** traffic through a VPN should include the possibility of this policy endangering other enclaves not party to the VPN.

4.3 ADDITIONAL RESEARCH REQUIRED

This interim guidance does not cover a variety of known port and protocol combinations such as those used by collaboration tools. Future guidance will address such items as research progresses.

5 GUIDELINES FOR TECHNICAL GUIDANCE DEVELOPMENT

5.1 GOALS.

The goal is to balance three equities for the NIPRNET:

- Security - recognizing the need to establish an acceptable level of shared NIPRNET community risk.
- Systems integration - recognizing the need to provide predictability for developers in development of interoperable DoD applications/systems by providing program managers predictable perimeter defense conditions through PPS standards.
- Inter-service Interoperability - recognizing the need to ensure that applications approved by the PPMP will be allowed to communicate through all boundary protection perimeters using the PPS required.

5.2 SECURITY.

To ensure an acceptable NIPRNET community risk is maintained, this technical guidance prescribes the following principles:

- A policy of Deny-by-default. Any PPS not specifically addressed in this guidance shall have a policy of "Deny."
- Any PPS too risky to be used shall have a policy of "Deny" and be designated as ***Red***. ***Red*** PPS's should not be used between NIPRNET users or between established security enclaves. No new implementations or systems shall use ***Red*** designated PPS's. Organizations with existing or legacy applications using such Red PPS's shall migrate their systems by redesign or replacement to eliminate the flow of the high risk ***Red*** PPS across the NIPRNET.
- PPS with associated risk, but operationally necessary, shall have a policy of "Conditional, Deny, or Allow," require specific security countermeasures to be invoked, and shall be designated as ***Yellow***.
- PPS with acceptable security characteristics shall have a policy of "Conditional, Deny, or Allow" and shall be designated as ***Green***.

5.3 RISK DESIGNATIONS (COLOR CODES)

Here are descriptions of the basis for technical security analysis for PPS for each of the three general risk designations, ***Red***, ***Yellow***, and ***Green***.

5.3.1 Red

PPSs designated as having unacceptably high risk for use across the NIPRNET. These PPSs are those services that have been determined to have exploitable vulnerabilities that may permit a remote attack, or reveal information regarding the network architecture. ***Red*** risk designation is also applied to services that are no longer used because the functionality is provided by a more secure service. Additionally, there are no known acceptable mitigation strategies to reduce the risk to an acceptable level. This designation serves as a guide to the acquisition community and to developers of the services that shall ***not*** be used in developing applications for use across the DII. The information in Section 0 is based on evaluations of the combination of port and data service. While the basic guidelines include the logic to block or deny any PPS not listed in the table, there are a number of known, well-defined services with significant vulnerabilities. These are included in Section 0 as explicit ***Red*** (Deny all) listings to preclude the inadvertent implementation by a new COTS or GOTS application on the NIPRNET.

5.3.2 YELLOW

PPSs with a known level of risk and an acceptable available risk mitigation strategy: These PPSs shall be used when there is a current operational requirement between enclaves as evaluated in the PPMP process. Risk mitigation conditions levied against these PPS will include required boundary protection device configuration. Specific security countermeasures shall be invoked as standard policy statements.

5.3.3 GREEN

PPSs designated as representing best security practices and advocated for use in future applications. These are PPS that meet all enforceable existing and future DoD and service policies and have an acceptable risk. Migration to these PPSs is desired and will result in a lower risk.

5.4 PORT REDIRECTION

Port redirection inside enclaves, not visible on the NIPRNET, is outside the scope of this guidance. The initial collection of ports and protocols listed in Section 0 includes those recognized as Well Known Ports and Registered Ports, as well as Private Ports known to members of the technical working group. In general, recognized data services should operate on their accepted Well Known (system) ports. However, the technical working group recognized that system architects sometimes use alternate non-standard port assignments. In the future these PPS combinations must be registered in the PPMP.

5.5 SELECTED MITIGATION TECHNIQUES

There are a wide variety of mitigation techniques that system architects and security engineers may use. Here are discussions of aspects of some of those techniques that may assist users of this document in understanding the use or value of them, relative to the vulnerabilities. Mitigation techniques are required to reduce the risk of vulnerable PPS. Guidance on which techniques should be used with a particular PPS combination is provided in the "conditions" column of the technical guidance table located in Section 0 and at http://www.cert.smil.mil.

5.5.1 USER AUTHENTICATION.

Advanced technology firewalls are available which integrate user authentication into the boundary protection process. When a connection is attempted, an associated user authentication can be required to allow the communication. The authentication can be integrated with network operating system passwords, with a PKI system, or with firewall-specific passwords.

5.5.2 CONNECTION CONTROL BY IP ADDRESS OR NETWORK.

Packets can be filtered based upon the source or destination machine IP address. Specification can be for the IP address of a single machine, or by network specification for a range of IP addresses. IP address restrictions can be stated by data layer Protocol (TCP or UDP, for example), or by specific ports to allow or deny. This technique limits the hosts from which data communications are accepted. This technique is not 100% effective. It is possible to construct packets, which have the IP address of a different machine (IP spoofing).

5.5.3 AUTHENTICATION BY DNS AND REVERSE ADDRESS RESOLUTION.

The Domain Name Service is a widely distributed database, maintained by a variety of authorities. In its current configuration, it is vulnerable to hostile corruption. For

that reason, using DNS and reverse address resolution as a means of authenticating remote systems is a weak mitigation technique.

5.5.4 DEMILITARIZED ZONES (DMZ)

A DMZ is a useful tool for operating servers, which routinely provide data on request to users outside of the operator's enclave. Web servers (http and https) and ftp servers are examples of services especially suited to placement in a DMZ instead of inside the principal enclave. One good policy for enclave boundary security is that all connections across the boundary must be initiated by an internal system. However, web servers and ftp servers always participate in connection sessions initiated from outside their own enclave. By placing these servers in a DMZ that allows externally initiated connections, the security manager can continue to enforce the policy of only allowing internally initiated sessions for all other systems, while allowing the web and ftp servers to operate as designed.

For example, the management of ftp servers requires additional consideration. In the default configuration for ftp services, the user (client) system initiates the ftp session on the control port, but the server initiates the actual file transfer on the data port. This is referred to as the user being in passive mode. However, since the user systems are all inside enclaves that should be enforcing the internally initiated connection rule, none of the users would be able to connect to the servers. Therefore, ftp systems should be configured for the users (clients) to all operate in active data transfer process mode. When so configured, the user (client) system not only initiates the control session with the server, but it also initiates the data transfer connection on the data port. As described above, this requires ftp servers to be operating in DMZ networks, which will allow the externally initiated data connection from the user.

5.5.5 INTERNET CONTROL MESSAGE PROTOCOL (ICMP) CONFIGURATION

Internet Control Message Protocol (ICMP) messages are required for proper functioning of the IP network layer. It is appropriate to block ICMP message types at the perimeter to reduce visibility of the protected network. Block any message types not required. Allow only the message types listed in the table at Section 0 to transit boundary protection devices. Note the direction of the request to be allowed.

6 ASSUMPTIONS

Services are assumed to adhere to standard Internet Assigned Numbers Authority (IANA) ports, unless otherwise stated. Services submitted for approval will identify the ports and protocols being used.

These requirements are not to conflict with the Intelligence Community's (IC) Open Source Information System (OSIS) firewall requirements. In cases where a conflict is noted, connectivity to C2 and Intelligence, Surveillance & Reconnaissance (ISR) systems will not be terminated. Migration to approved PPSs will be worked as part of the PPMP.

The DoD Mobile Code Policy Memorandum addresses services that utilize mobile code technologies.

Service and Agency internal PPS will be registered on the DoD registry however, services will have separate approval authority for service internal PPS. The Service Designated Approval Authority (DAA) will have sole approval authority for internal PPS use.

Network layer tunneling protocols that obscure protocol and port information, as well as data from Intrusion Detection Systems (IDS) and firewalls, require special treatment:

Transport layer and application layer encryption/tunneling are not as objectionable because it does not have the capability to carry the full range of attacks of network layer tunneling protocols.

Other DoD policy applies to tunneling methods used to protect sensitive unclassified and national security related data.

7 ACRONYMS

AIS	Automated Information System
C/S/A	CINC/Service/Agency
C2	Command & Control
CCB	Configuration Control Board
CINC	Commander in Chief
CND	Computer Network Defense
COTS	Commercial Off The Shelf
DII	Defense Information Infrastructure
DMZ	Demilitarized Zone
FAA	Federal Aviation Administration
GOTS	Government Off The Shelf
IA	Information Assurance
IANA	Internet Assigned Numbers Authority
IC	Intelligence Community
ICMP	Internet Control Messaging Protocol
IDS	Intrusion Detection Systems
IETF	Internet Engineering Task Force
ISR	Intelligence, Surveillance & Reconnaissance
LAN	Local Area Network
OSIS	Open Source Information System
PPMP	Ports & Protocols Management Process
PPS	Port, Protocol, and Service
RFC	Request for Comment
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
USCG	United States Coast Guard
VPN	Virtual Private Network
WAN	Wide Area Network

8 GLOSSARY

Access Control - The process of limiting access to the resources of a system only to authorized programs, processes, or other systems (in a network). Synonymous with controlled access and limited access.

Allow - A firewall rule set that permits traffic to transit the network boundary, regardless of the protocol being used, to communicate from one host (source) to another (destination).

Application - For information assurance purposes, an application is the product or deliverable of an Automated Information System (AIS) acquisition program as defined by DoDD 5000.1. An application performs clearly defined functions for which there are readily identifiable security considerations and needs are addressed as part of the acquisition. An application may be a single software application; multiple individual applications that are related to a single mission function (e.g., payroll or personnel); or a combination of software and hardware focused on supporting a specific mission-related function. Applications are deployed to enclaves for operations, and have their operational security needs assumed by the enclave. Note. An application is analogous to a "major application" as defined in NIST Special Pub 800-18 (reference (z)); however, this term is not used in order to avoid confusion with the DoD acquisition category of Major Automated Information System (MAIS).

Approval - The formal process of enrolling the desired use of a protocol and its associated port number(s) on DoD networks.

Attack - The act of trying to bypass security controls on a system. An attack may be active, resulting in the alteration of data; or passive, resulting in the release of data. The degree of success depends on the vulnerability of the system or activity and the effectiveness of existing countermeasures. The intentional act of attempting to bypass security controls on an automated information system (AIS).

Authorization - The process of checking the rights (or permissions) to the server resource that are allowed for the subject; for example, a subject might be allowed read access but not write access to a server resource.

Centralized Management - The concept of using a single, designated management authority. It includes system management, program and project management, and product management.

Certification - The process of determining the effectiveness of all security mechanisms. The comprehensive evaluation of the technical and non-technical security features of an AIS and other safeguards, made in support of the accreditation process, that establishes the extent to which a particular design and implementation meet a specified set of security requirements.

Conditional - This is a firewall rule set that is denied by default, but may be allowed when implemented under additional considerations. Such consideration may require specific architectural implementation or the use of additional software to help mitigate some risks inherent within those protocols and services.

Configuration - A collection of an item's descriptive and governing characteristics, which can be expressed in functional terms, i.e., what performance the item is expected to achieve; and in physical terms, i.e., what the item should look like and consist of when it is built.

Deconfliction - The process to identify and resolve the issues related to any conflicting use of a protocol and its associated port number(s) on DoD networks.

Defense Information Infrastructure (DII) - The shared or interconnected system of computers, communications, data applications, security, people, training and other support structures serving DoD local, national, and worldwide information needs. DII connects DoD mission support, command and control, and intelligence computers through voice, telecommunications, imagery, video, and multimedia services. It provides information processing and services to the subscribers over the Defense Information Systems Network (DISN) and includes command and control, tactical, intelligence, and commercial communications systems used to transmit DoD information.

Demilitarized Zone (DMZ) - A subnet that is logically between internal and external networks. Its purpose is to enforce the internal network's IA policy for external information exchange and to provide external, untrusted sources with restricted access to releasable information while shielding the internal networks from outside attacks. A DMZ is also called a 'screened subnet.'

Deny - A firewall rule set that does NOT permit traffic to transit a network boundary across a giving port. Protocols or services that commonly use these ports have been determined to pose a significant threat to the protected network. Therefore the protocol is not allowed for to enter the protected enclave from an untrusted enclave.

DoD Information System - A general term used to refer to an application, an enclave, an outsourced IT-based process, or platform IT interconnection.

Enclave - For information assurance purposes, an enclave is a collection of computing environments that is connected by one or more internal networks and is under the control of a single authority and security policy, including personnel and physical security. Enclaves have readily identifiable security needs, provide common IA capabilities, and are analogous to general support systems as defined in NIST Special Pub 800-18 (reference (z)). Enclaves may be specific to an organization or a mission. They may be sites that are based on physical location and proximity or they may be logical. Examples of enclaves include local area networks and the applications they host, backbone networks, and data processing centers.

Enforcement - A collaborative process to monitor and control the use of a protocol and its associated port number(s) on DoD networks.

Firewall - A system or combination of systems that enforces a boundary between two or more networks. A gateway that limits access between networks in accordance with local security policy.

Internet Assigned Numbers Authority (IANA) - See http://www.iana.org/.

Internet Engineering Task Force (IETF) - The cooperative organization that coordinates and sets standards for the Internet. See http://www.ietf.org/.

Inbound - A TCP/UDP connection that originates from outside the enclave to inside the enclave.

Information Assurance (IA) - Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

Internet Control Messaging Protocol (ICMP) - See IETF RFC 792.

Legacy Systems - Systems that are candidates for phase-out, upgrade, or replacement. Generally legacy systems are in this category because they do not comply with data standards or other standards. Legacy system workloads must be converted, transitioned, or phased out.

Local Area Network (LAN) - A local network of users, systems, wiring, switching, and ancillary devices which is established under a single administrative control to provide network services. A LAN is typically no larger than a single building. When several LANs are interconnected under a single broad administrative control they form a Campus Area Network (CAN) or a Metropolitan Area Network (MAN). A CAN or MAN is normally the largest increment of a network that does not require WAN connections to communicate between elements.

Non-Classified Internet Protocol Router Network (NIPRNET) - The data communications component of the DISN used for unclassified but sensitive data.

Outbound - A TCP/UDP connection that originates from inside the enclave to outside the enclave.

Port - A logical point of connection, most especially in the context of TCP (Transmission Control Protocol) and UDP (User Datagram Protocol), which is part of the TCP/IP protocol suite developed for what we now know as the Internet. As recorded with IANA, ports are identified as being in three categories: Well-Known Ports, Registered Ports, and Private or Dynamic Ports. The System (Well-Known) Ports are those from 0 through 1023. The User (Registered) Ports are those from 1024 through 49151. The Dynamic and/or Private Ports are those from 49152 through 65535. See http://www.iana.org/assignments/port-numbers.

Port Number - In Internet protocol networks, such as the Internet and DoD's NIPRNET and SIPRNET, a port is an integer number assigned to a logical network service to differentiate and direct appropriate requests, contained in incoming traffic, to that specific service running on a host computer.

Port Redirection - System architects sometimes choose to use a known application service on a numbered port other than the well-known port. The router, firewall, or proxy at the enclave boundary will redirect packets recognized as appropriate to an alternate port on the target system inside the enclave.

Protocol - Agreed-upon methods of communications used by computers. A specification that describes the rules and procedures that products should follow to perform activities on a network, such as transmitting data. If they use the same protocols, products from different vendors should be able to communicate on the same network. Within the context of this document, protocol refers to the Internet protocols numbered 0 to 255 listed in IANA, found on the Web at http://www.iana.org/assignments/protocol-numbers. Their use is described in [RFC952]

Protocol Services - Any function performed by a protocol for example send, receive, routing, etc.

Request for Comment (RFC) - The standard publication used by the IETF to publish proposed and finalized standards for the Internet. See http://www.ietf.org/rfc.html.

Relay - Any device that does not provide a direct line of communications through the firewall (e.g., secure server).

Risk Assessment - The process of identifying program risks within risk areas and critical technical processes, analyzing them for their consequences and probabilities of occurrence, and prioritizing them for handling.

Service - A process or application that runs on a server and provides some benefit to a network user. In the IANA listing of ports at http://www.iana.org/assignments/port-numbers the Service (as used here) is referred to as a server process, and is identified by a Keyword (e.g. ftp) and a Description (e.g. File Transfer). Note that many server processes or services use the word "protocol" in their name. It is important to be clear in context when "protocol" refers to an Internet Protocol (e.g. TCP) or is part of the name of a service.

System - The organization of hardware, software, material, facilities, personnel, data, and services needed to perform a designated function with specified results, such as the gathering of specified data, its processing, and delivery to users. 2. A combination of two or more interrelated pieces of equipment (sets) arranged in a functional package to perform an operational function or to satisfy a requirement.

Transmission Control Protocol (TCP) - See IETF RFC793.

Threat - The means through which the ability or intent of a threat agent to adversely affect an automated system, facility, or operation can be manifest. A potential violation of security.

User Datagram Protocol (UDP) - See IETF RFC768.

Virtual Private Network (VPN) - a physically disparate set of networks that share a common security perimeter and policy through secured internetwork communication.

Vulnerability - A weakness in automated system security procedures, administrative controls, physical layout, internal controls, and so forth, that could be exploited by a threat to gain unauthorized access to information or disrupt critical processing.

Vulnerability Assessment - Systematic examination of an AIS or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation in a network-centric environment.

Wide Area Network (WAN) - A physical or logical network that provides capabilities for a number of independent devices to communicate with each other over a common transmission-interconnected topology in geographic areas larger than those served by local area networks. The Internet and DoD's NIPRNET are examples of a WAN.

9 DESIGNATED PORTS, PROTOCOLS AND SERVICES

ICMP Messages

ICMP Message Number	ICMP Message name	Configuration recommendation
0	Echo Reply	Allow outbound only
3	Destination Unreachable	Allow outbound only
4	Source Quench	Allow both directions
8	Echo Request	Allow outbound only
11	Time exceeded	Allow inbound only
12	Parameter problem	Allow both directions

TCP/UDP Services

Services	Ports	Prot	Designation	Policy		Conditions		Comments
				In	Out	In	Out	
Reserved	0	TCP	Red	Deny	Deny			
Reserved	0	UDP	Red	Deny	Deny			
TCPMux	1	TCP UDP	Red	Deny	Deny			
Remote Job Entry	5	TCP, UDP	Red	Deny	Deny			
Echo	7	TCP; UDP	Red	Deny	Deny			See CERT/CC 96-01 Denial of Service
Discard	9	TCP; UDP	Red	Deny	Deny			
Systat	11	TCP UDP	Red	Deny	Deny			
Daytime	13	TCP; UDP	Red	Deny	Deny			See CERT/CC 96-01 Denial of Service
Netstat	15	TCP UDP	Red	Deny	Deny			
qotd	17	TCP; UDP	Red	Deny	Deny			
MSP, v2	18	TCP	Red	Deny	Deny			
Chargen	19	TCP; UDP	Red	Deny	Deny			See CERT/CC 96-01 Denial of Service (UDP)
FTP-(passive Data Transfer Process at client)	20,21	TCP	Red	Deny	Deny	- Deny	- Deny	When the ftp system (whether server or user (client) inside an enclave allows the external ftp system to initiate data transfer on the data port, then it is not possible for the enclave firewall to establish a session record initiated by a known internal system. See the discussion of DMZ usage for ftp and http servers.

Services	Ports	Prot	Designation	Policy		Conditions		Comments
				In	Out	In	Out	
FTP-(active Data Transfer Process at client)	20,21	TCP; UDP	Yellow	Deny	Allow	- Deny	- Allow	In order for firewalls to establish session records based on internal initiators, all ftp data transfer sessions must begin from inside the enclave. This requires the ftp user system in the enclave to operate in active DTP mode, sending the PASV command to the server. See the discussion of DMZ usage for ftp and http servers.
								FTP is well known in the security community to be a highly vulnerable data service. The advisory committee also recognizes that it is a central data service to a large number of essential AIS implementations in DoD. AIS managers who rely on raw telnet are strongly urged to engineer replacement data communication processes of higher security as soon as possible.
SSH	22	TCP	Yellow	Cond	Allow	- Allow inbound to only authorized servers	- Allow	
Telnet	23	TCP	Yellow	Cond	Allow	- Allow inbound to only authorized servers - Allow outbound from only authorized servers - Strong Authentication - Relay	- Allow	Telnet is well known in the security community to be a highly vulnerable data service. The advisory committee also recognizes that it is a central data service to a large number of essential AIS implementations in DoD. AIS managers who rely on raw telnet are strongly urged to engineer replacement data communication processes of higher security as soon as possible.
SMTP	25	TCP	Yellow	Cond	Cond	- Allow inbound to only authorized servers	- Relay	
Time	**37**	**TCP; UDP**	**Red**	**Deny**	**Deny**			**See CERT/CC 96-01 Denial of Service (UDP).**
Whois	43	**TCP; UDP**	**Red**	**Deny**	**Deny**			
Nickname (whois)	47	TCP	Yellow	Deny	Deny	permit to specific server, relay		Network and security administrators require access to whois information.
Login host protocol	49	TCP	Yellow	Cond	Cond	TACACS Plus to secure password	TACACS Plus to secure password	RFC 1700 TACACS
RE-Mail-CK	**50**	**TCP; UDP**	**Red**	**Deny**	**Deny**			

Services	Ports	Prot	Designation	Policy		Conditions		Comments
				In	Out	In	Out	
DNS	53	TCP;	Yellow	Cond	Cond	- source/destination IP restricted - Relay - split-DNS	- source/destination IP restricted - Relay - split-DNS	
DNS	53	UDP	Yellow	Cond	Cond	- Relay	- Relay	
DNSSEC	53	TCP; UDP	Green	Deny	Cond	- Deny	- Relay	
Bootps	**67**	**TCP; UDP**	**Red**	**Deny**	**Deny**			
Bootpc	**68**	**TCP; UDP**	**Red**	**Deny**	**Deny**			
Tftp	**69**	**TCP/ UDP**	**Red**	**Deny**	**Deny**			
Gopher	70	TCP	Yellow	Deny	Cond	- Deny	- Restrict to destination domain	Used to access the Congressional Gopher Server
NETRJS	**71-74**	**TCP; UDP**	**Red**	**Deny**	**Deny**			
Finger	**79**	**TCP**	**Red**	**Deny**	**Deny**			See CERT/CC Advisory 93-04 and DOD CERT Bulletin 93-06.
HTTP	80	TCP	Green	Deny	Cond	- Deny	- Relay Place http servers in DMZ	Require the use of application layer proxy to more effectively control the use of this protocol.
LINK	**87**	**TCP**	**Red**	**Deny**	**Deny**			
Kerberos	88	TCP/ UDP	Yellow	Cond	Cond	- source/destination IP restricted	- source/destination IP restricted	
Supdup	**95**	**TCP**	**Red**	**Deny**	**Deny**			
Hostname	**101**	**TCP**	**Red**	**Deny**	**Deny**			
MTA	102		Yellow	Cond	Cond	- Allow inbound to only authorized servers	- Restrict by Source IP - Restrict by Destination IP - NAT off	
X.500	102	TCP	Yellow	Cond	Cond	- Allow inbound to only authorized servers	- Restrict by Source IP - Restrict by Destination IP - NAT off	
X.400	104	TCP	Yellow	Cond	Cond	- Allow inbound to only authorized servers	- Restrict by Source IP - Restrict by Destination IP - NAT off	
RTELNET	**107**	**TCP; UDP**	**Red**	**Deny**	**Deny**			
POP-2	**109**	**TCP**	**Red**	**Deny**	**Deny**			**See CERT/CC Advisory 98-11, 98-07, 97-09.**

Services	Ports	Prot	Designation	Policy		Conditions		Comments
				In	Out	In	Out	
POP-3	**110**	**TCP**	**Red**	**Deny**	**Deny**			
Sun RPC	111	TCP/ UDP	Yellow	Cond	Cond	- Restrict by Source IP Restrict by Destination IP	- Restrict by Source IP Restrict by Destination IP	Recommend implementing via VPN.
Auth	113	TCP	Red	Deny	Deny			See DOD CERT Bulletin 95-43
SFTP	115	TCP	Red	Deny	Deny			
UUCP-path	117	TCP	Red	Deny	Deny			See CERT/CC Advisory 92-06.
NNTP	119	TCP	Yellow	Cond	Cond	- Allow inbound to only authorized servers - DMZ	- Restrict by destination domain - Relay	
NTP	123	TCP/ UDP	Yellow	Cond	Cond	- Restrict by Source IP	- Restrict by destination domain	
Statsrv	133	TCP	Red	Deny	Deny			See CERT/CC Advisory 97-26 and DOD CERT Bulletin 96-12.
MS-RPC	135	TCP; UDP	Red	Deny	Deny			
NetBIOS	137-139	TCP; UDP	Red	Deny	Deny			
IMAP2	143	TCP	Red	Deny	Deny			See CERT/CC 98-11, 98-07.
SNMP	161	TCP/ UDP	Yellow	Cond	Cond	- Restrict by Source IP - Restrict by Destination IP	- Restrict by Source IP - Restrict by Destination IP	Consider authentication by community string IAW DoD password guidance Change community string to other than "public" or "private"
SNMPTRAP	162	TCP/ UDP	Yellow	Cond	Cond	- Restrict by Source IP - Restrict by Destination IP	- Restrict by Source IP - Restrict by Destination IP	
XDMCP	177	TCP;UDP	Red	Deny	Deny			
Border Gateway Protocol	179	TCP/ UDP	Red	Deny	Deny			As a routing protocol, should never pass through an enclave boundary
IRC	194	TCP	Red	Deny	Deny			See CERT/CC Advisory 94-14 and DOD CERT Bulletin 93-33.
IMAP3	220	TCP	Red	Deny	Deny			See CERT/CC Advisory 98-11, 98-07, 97-09.
ICI (CMOS Interactive Communications Interface)	251	TCP	Yellow	Cond	Cond	- Restrict by Destination IP	- Restrict by Destination IP	CMOS Interactive Communications Interface.
InfoConnect	256	TCP	Yellow	Cond	Cond		- Restrict by Destination IP	
LDAP	389	TCP	Yellow	Cond	Allow	- Allow inbound to only authorized servers	- Allow	

Services	Ports	Prot	Designation	Policy		Conditions		Comments
				In	Out	In	Out	
LDAP	390	TCP	Yellow	Cond	Allow	- Allow inbound to only authorized servers	- Allow	
HTTPS	443	TCP	Green	Cond	Cond	- Allow inbound to only authorized servers	- Relay	SSL & TLS implementation for http
Microsoft DS	445	TCP/ UDP	Red	Deny	Deny	-		
IPSEC Negotiation	500	UDP	Yellow	Cond	Cond	- Allow inbound to only authorized servers	- Restrict by Source IP - Restrict by Destination IP	
Rexec	512	TCP	Red	Deny	Deny			See CERT/CC Advisories 97-06, 95-15, 94-09.
Rlogin	513	TCP	Red	Deny	Deny			
Rwho	513	UDP	Red	Deny	Deny			
Rsh	514	TCP	Red	Deny	Deny			
Syslog	514	UDP	Yellow	Cond	Cond	- Allow inbound to only authorized servers	- Restrict by Destination IP	
LPD (Printing) LPR	515	TCP	Yellow	Cond	Cond	- Allow inbound to only authorized servers	- Encrypted over the WAN - Transition	Line printer spooler. See CERT/CC Advisories 97-19, 95-15. Defense Integrated Management Engineering System (DIMES)
Talk	517	UDP	Red	Deny	Deny			See CERT/CC Advisory 97-04 and DOD CERT Bulletin 97-07.
Ntalk	518	UDP	Red	Deny	Deny			
RPC	530	TCP; UDP	Red	Deny	Deny			
UUCP	540	TCP	Red	Deny	Deny			See CERT/CC Advisory 92-06.
UUCP	541	TCP; UDP	Red	Deny	Deny			
Kshell	544	TCP/ UDP	Yellow	Cond	Cond	permit from specific clients/ permit to specific servers/	No NAT	
NNTP(SSL)	563	TCP	Green	Deny	Cond	- Allow inbound to only authorized servers - DMZ	- Restrict by destination domain - Relay	nntp protocol over TLS/SSL (was snntp)
NNTP(SSL)	563	UDP	Green	Deny	Cond	- Allow inbound to only authorized servers - DMZ	- Restrict by destination domain - Relay	nntp protocol over TLS/SSL (was snntp)
Ipp	631	TCP	Green	Cond	Cond	Restrict by Source IP Restrict by Destination IP	Restrict by Source IP Restrict by Destination IP	IPP (Internet Printing Protocol)
Ipp	631	UDP	Green	Cond	Cond	Restrict by Source IP Restrict by Destination IP	Restrict by Source IP Restrict by Destination IP	IPP (Internet Printing Protocol)

Services	Ports	Prot	Designation	Policy		Conditions		Comments
				In	Out	In	Out	
LDAPS	636	TCP; UDP	Green	Deny	Cond	- Deny	- Allow	LDAP protocol over TLS/SSL (was sldap).
LDAPS	637	TCP; UDP	Green	Deny	Cond	- Deny	- Allow	LDAP protocol over TLS/SSL (was sldap).
Kerberos kerberos-adm	749	TCP, UDP	Yellow	Deny	Deny	permit from specific clients	- permit to specific servers	No NAT
ftps-data	989	TCP	Green	Cond	Allow	Restrict by Source IP Restrict by Destination IP	- Allow	ftp protocol, data, over TLS/SSL
ftps-data	989	UDP	Green	Cond	Allow	Restrict by Source IP Restrict by Destination IP	- Allow	ftp protocol, data, over TLS/SSL
Ftps	990	TCP	Green	Cond	Allow	Restrict by Source IP Restrict by Destination IP	Allow	ftp protocol, control, over TLS/SSL
Ftps	990	UDP	Green	Cond	Allow	Restrict by Source IP Restrict by Destination IP	Allow	ftp protocol, control, over TLS/SSL
Telnets	992	TCP	Green	Cond	Cond	Restrict by Source IP Restrict by Destination IP	Restrict by Source IP Restrict by Destination IP	telnet protocol over TLS/SSL
telnets	992	UDP	Green	Cond	Cond	Restrict by Source IP Restrict by Destination IP	Restrict by Source IP Restrict by Destination IP	telnet protocol over TLS/SSL
IMAP(SSL)	993	TCP	Green	Cond	Cond	- Allow inbound to only authorized servers	- Restrict by destination domain - Relay	
Ircs	994	TCP	Green	Cond	Cond	Restrict by Source IP Restrict by Destination IP	Restrict by Source IP Restrict by Destination IP	irc protocol over TLS/SSL
Ircs	994	UDP	Green	Cond	Cond	Restrict by Source IP Restrict by Destination IP	Restrict by Source IP Restrict by Destination IP	irc protocol over TLS/SSL
POP3(SSL)	995	TCP	Green	Cond	Cond	- Allow inbound to only authorized servers	- Restrict by destination domain - Relay	
netspy	**1024**	**TCP**	**Red**	**Deny**	**Deny**			
Listener Rasmin	**1025**	**TCP**	**Red**	**Deny**	**Deny**			
Aventail	1080	TCP	Yellow	Cond	Cond	- Allow inbound to only authorized servers	- Restrict by Source IP - Restrict by Destination IP	* DISA Ogden
Xtreme	**1090**	**TCP**	**Red**	**Deny**	**Deny**	-		
ISOIPSIGPORT-1	1106	TCP	Yellow	Cond	Cond	- Allow inbound to only authorized servers	- Restrict by Source IP - Restrict by Destination IP	* DISA Ogden
ISOIPSIGPORT-2	1107	TCP	Yellow	Cond	Cond	- Allow inbound to only authorized servers	- Restrict by Source IP - Restrict by Destination IP	* DISA Ogden

Services	Ports	Prot	Designation	Policy		Conditions		Comments
				In	Out	In	Out	
	1137		Yellow	Cond	Cond	- Allow inbound to only authorized servers	- Restrict by Source IP - Restrict by Destination IP	* US ARMY at Ft Monroe
Lightspeed Print	1138	UDP	Yellow	Cond	Cond	- Allow inbound to only authorized servers	- Restrict by Source IP - Restrict by Destination IP	* US ARMY at Ft Monroe
Psyber S.S.	1170	**TCP**	**Red**	**Deny**	**Deny**	-		
Caiccipc ???	1202	TCP	Yellow	Cond	Cond	- Allow inbound to only authorized servers	- Restrict by Source IP - Restrict by Destination IP	* DLA Columbus
Ultors Trojan	1234	**TCP**	**Red**	**Deny**	**Deny**	-		
VooDoo Doll	1245	**TCP**	**Red**	**Deny**	**Deny**	-		
Back Orifice DLL	1349	UDP	**Red**	**Deny**	**Deny**	-		
Editbench ???	1350	TCP	Yellow	Cond	Cond	- Allow inbound to only authorized servers	- Restrict by Source IP - Restrict by Destination IP	* DISA Mechanicsburg
Lotusnotes	1352	TCP	Yellow	Cond	Cond	- Restrict by Source IP - - Restrict by Destination IP	- Restrict by Source IP - Restrict by Destination IP	
Cuillamartin ???	1356	TCP	Yellow	Cond	Cond	- Allow inbound to only authorized servers	- Restrict by Source IP - Restrict by Destination IP	* DSIS Application at DMC Mechanicsburg
Connlcli ???	1358	TCP	Yellow	Cond	Cond	- Allow inbound to only authorized servers	- Restrict by Source IP - Restrict by Destination IP	* DSIS Application at DMC Mechanicsburg
Mimer ???	1360	TCP	Yellow	Cond	Cond	- Allow inbound to only authorized servers	- Restrict by Source IP - Restrict by Destination IP	* DSIS Application at DMC Mechanicsburg
SNA	1365	TCP	Yellow	Cond	Cond	- Allow inbound to only authorized servers	- Restrict by Source IP - Restrict by Destination IP	* various DISA and DFAS locations
Screencast ???	1368	TCP	Yellow	Cond	Cond	- Allow inbound to only authorized servers	- Restrict by Source IP - Restrict by Destination IP	* DSIS Application at DMC Mechanicsburg
SQL Server	1433	TCP	Yellow	Cond	Cond	- Allow inbound to only authorized servers	- Restrict by Source IP - Restrict by Destination IP - Relay	
FTP99CMP	1492	TCP	**Red**	**Deny**	**Deny**			
ICA	1494	TCP	Yellow	Cond	Cond	- Allow inbound to only authorized servers	- Restrict by Source IP - Restrict by Destination IP	
MS NetMtg	1503	TCP	Yellow	Cond	Allow	- Allow inbound to only authorized servers	- Allow	- Allow
Ifor-protocol	1515	TCP/ UDP	?			-	-	
SQL Listener	1521	TCP	Yellow	Cond	Cond	- Allow inbound to only authorized servers	- Restrict by Source IP - Restrict by Destination IP	* DISA and other agencies

Services	Ports	Prot	Designation	Policy		Conditions		Comments
				In	Out	In	Out	
SQL*Net	1521	TCP	Yellow	Cond	Cond	- Allow inbound to only authorized servers	- Restrict by Source IP - Restrict by Destination IP - Relay	
Interpid (Oracle)	1521	TCP	Yellow	Cond	Cond	- Allow inbound to only authorized servers	- Restrict by Destination IP	CAC Common Access Cards - USMC (added 30 March 2001)
Oracle	1521	TCP	Yellow	Cond	Cond	- Allow inbound to only authorized servers	- Restrict by Destination Domain - Requires Transition	DEERS/RAPIDS ID - USMC (added 30 March 2001)
SQL*Net	1522	TCP	Yellow	Cond	Cond	- Allow inbound to only authorized servers	- Restrict by Destination IP - Relay	
SQL Listener	1523	TCP	Yellow	Cond	Cond	- Allow inbound to only authorized servers	- Restrict by Destination IP - Relay	* AF El Segundo
SQL*Net	1525	TCP	Yellow	Cond	Cond	- Allow inbound to only authorized servers	- Restrict by Destination IP - Relay	
SQL*Net v.2	1526	TCP	Yellow	Cond	Cond	- Allow inbound to only authorized servers	- Restrict by Destination IP - Relay	
SQL Listener	1526	TCP	Yellow	Cond	Cond	- Allow inbound to only authorized servers	- Restrict by Destination IP - Relay	* AF Eglin, AF Elmendorf, AF Hickam, AF El Segundo, DISA Huntsville, DISA Rock Island, DECA
SQL Listener	1527	TCP	Yellow	Cond	Cond	- Allow inbound to only authorized servers	- Restrict by Destination IP - Relay	* DISA Huntsville
SQL Listener	1528	TCP	Yellow	Cond	Cond	- Allow inbound to only authorized servers	- Restrict by Destination IP - Relay	* DISA Huntsville
SQL Listener	1529	TCP	Yellow	Cond	Cond	- Allow inbound to only authorized servers	- Restrict by Destination IP - Relay	* DISA Huntsville
SQL Listener	1532	TCP	Yellow	Cond	Cond	- Allow inbound to only authorized servers	- Restrict by Destination IP - Relay	* DISA Huntsville
SQL Listener	1533	TCP	Yellow	Cond	Cond	- Allow inbound to only authorized servers	- Restrict by Destination IP - Relay	* DISA Huntsville
SQL Listener	1534	TCP	Yellow	Cond	Cond	- Allow inbound to only authorized servers	- Restrict by Destination IP - Relay	* DISA Huntsville
SQL Listener	1535	TCP	Yellow	Cond	Cond	- Allow inbound to only authorized servers	- Restrict by Destination IP - Relay	* DISA Huntsville
DD/AM	1541	TCP	Yellow	Cond	Cond	- Allow inbound to only authorized servers	- Restrict by Source IP - Restrict by Destination IP	* DISA Mechanicsburg runs a Document Direct / Access Mechanism
DD/AM	1542	TCP	Yellow	Cond	Cond	- Allow inbound to only authorized servers	- Restrict by Source IP - Restrict by Destination IP	* DISA Mechanicsburg runs a Document Direct / Access Mechanism
DD/AM	1543	TCP	Yellow	Cond	Cond	- Allow inbound to only authorized servers	- Restrict by Source IP - Restrict by Destination IP	* DISA Mechanicsburg runs a Document Direct / Access Mechanism

Services	Ports	Prot	Designation	Policy		Conditions		Comments
				In	Out	In	Out	
DD/AM	1544	TCP	Yellow	Cond	Cond	- Allow inbound to only authorized servers	- Restrict by Source IP - Restrict by Destination IP	* DISA Mechanicsburg runs a Document Direct / Access Mechanism
DD/AM	1545	TCP	Yellow	Cond	Cond	- Allow inbound to only authorized servers	- Restrict by Source IP - Restrict by Destination IP	* DISA Mechanicsburg runs a Document Direct / Access Mechanism
DD/AM	1546	TCP	Yellow	Cond	Cond	- Allow inbound to only authorized servers	- Restrict by Source IP - Restrict by Destination IP	* DISA Mechanicsburg runs a Document Direct / Access Mechanism
DD/AM	1548	TCP	Yellow	Cond	Cond	- Allow inbound to only authorized servers	- Restrict by Source IP - Restrict by Destination IP	* DISA Mechanicsburg runs a Document Direct / Access Mechanism
DD/AM	1561	TCP	Yellow	Cond	Cond	- Allow inbound to only authorized servers	- Restrict by Source IP - Restrict by Destination IP	* DISA Mechanicsburg runs a Document Direct / Access Mechanism
DD/AM	1562	TCP	Yellow	Cond	Cond	- Allow inbound to only authorized servers	- Restrict by Source IP - Restrict by Destination IP	* DISA Mechanicsburg runs a Document Direct / Access Mechanism
DD/AM	1575	TCP	Yellow	Cond	Cond	- Allow inbound to only authorized servers	- Restrict by Source IP - Restrict by Destination IP	* DISA Mechanicsburg runs a Document Direct / Access Mechanism
Shivka-Burka	1600	TCP	**Red**	**Deny**	**Deny**	-	-	
SQL*Net	1601	TCP	Yellow	Cond	Cond	- Allow inbound to only authorized servers	- Restrict by Destination IP - Relay	
Icabrowser	1604	TCP/ UDP	Yellow	Cond	Cond	Restrict by Source IP - - Restrict by Destination IP	Restrict by Source IP - - Restrict by Destination IP	
microcom-sbp ???	1680	TCP	Yellow	Cond	Cond	- Allow inbound to only authorized servers	- Restrict by Source IP - Restrict by Destination IP	* Cognos Cube publishing at DISA Columbus
PPTP	1723	TCP; UDP	Yellow	Cond	Cond	- Allow inbound to only authorized servers	- Requires Transition	DEERS/RAPIDS ID - USMC (added 30 March 2001)
SQL*Net	1748	TCP	Yellow	Cond	Cond	- Allow inbound to only authorized servers	- Restrict by Destination IP - Relay	
SpySender	1807	TCP	**Red**	**Deny**	**Deny**	-		
Shockrave	1981	TCP	**Red**	**Deny**	**Deny**	-		
stun-port ???	1994	TCP	Yellow	Cond	Cond	- Allow inbound to only authorized servers	- Restrict by Source IP - Restrict by Destination IP	* DISA Ogden and DFAS Cleveland
BackDoor	1999	TCP	**Red**	**Deny**	**Deny**	-		
lpxerox	2000	TCP	Yellow	Cond	Cond	- Allow inbound to only authorized servers	- Restrict by Source IP - Restrict by Destination IP	* DISA Huntsville
Trojan Cow	2001	TCP	**Red**	**Deny**	**Deny**	-		
Ripper	2023	TCP	**Red**	**Deny**	**Deny**	-		
EDI Viewer	2027	TCP	Yellow	Cond	Cond	- Allow inbound to only authorized servers	- Restrict by Source IP - Restrict by Destination IP	* DISA Ogden
EDI Viewer	2037	TCP	Yellow	Cond	Cond	- Allow inbound to only authorized servers	- Restrict by Source IP - Restrict by Destination IP	* DISA Ogden

Services	Ports	Prot	Designation	Policy		Conditions		Comments
				In	Out	In	Out	
NFS	**2049**	**TCP; UDP**	**Red**	**Deny**	**Deny**			**See CERT/CC Advisories 98-12, 96-09, 94-15, 94-02, 93-15, 92-15, 91-21, and DOD CERT Bulletin 1999-A-6, 1999-01, 94-41.**
Front End Processor	2065	TCP	Yellow	Cond	Cond	- Allow inbound to only authorized servers	- Restrict by Source IP - Restrict by Destination IP	* DISA Ogden, Chambersburg, Mechanicsburg
Bugs	**2115**	**TCP**	**Red**	**Deny**	**Deny**			
Deep Throat	**2140**	**TCP**	**Red**	**Deny**	**Deny**			
Subseven21	**2222**	**TCP**	**Red**	**Deny**	**Deny**			
compaqdiag	**2301**	**TCP; UDP**	**Red**	**Deny**	**Deny**			
Striker	**2565**	**TCP**	**Red**	**Deny**	**Deny**			
WinCrash	**2583**	**TCP**	**Red**	**Deny**	**Deny**			
Listen	**2766**	**TCP**	**Red**	**Deny**	**Deny**			
Phineas P.	2801	**TCP**	**Red**	**Deny**	**Deny**	-		
AHIPC	3002	TCP	Yellow	N/A	Cond	N/A (Client)	- Restrict by Destination IP - Requires Transition	DEERS/RAPIDS ID (Client) - USMC (added 30 March 2001)
Redberry-RIM	3101	TCP	Yellow	Deny	Cond		- Restrict by Destination IP - Restrict by Source IP	
Deskbook	3336	TCP	Yellow	Cond	Cond	- Allow inbound to only authorized servers	- Restrict by Source IP - Restrict by Destination IP	* DISA Ogden
	3389	TCP	Yellow	Cond	Cond	- Allow inbound to only authorized servers	- Restrict by Source IP - Restrict by Destination IP	* AF Randolph, DISA Ogden
SMARTPASS	3845	TCP	Yellow	Cond	Cond	- Allow inbound to only authorized servers	- Restrict by Source IP - Restrict by Destination IP	* DISA Ogden, NIPR (unknown)
BARS	3986	TCP	Yellow	Cond	Cond	- Allow inbound to only authorized servers	- Restrict by Source IP - Restrict by Destination IP	* AF Gunter, AF Crane
- Restrict by Destination IP								
AHIPC	4009	TCP	Yellow	Cond	Cond	- Allow inbound to only authorized servers	- Restrict by Destination Domain - Requires Transition	DEERS/RAPIDS ID (Server) - USMC (added 30 March 2001)
locksd	4045	**UDP**	**Red**	**Deny**	**Deny**	-		
DPAS	4610	TCP	Yellow	Cond	Cond	- Allow inbound to only authorized servers	- Restrict by Source IP - Restrict by Destination IP	* Navy Crane
DFAS Charleston	4610	TCP	Yellow	Cond	Cond	- Allow inbound to only authorized servers	- Restrict by Source IP - Restrict by Destination IP	* AF Crane
DPAS	5000	TCP	Yellow	Cond	Cond	- Allow inbound to only authorized servers	- Restrict by Destination IP	* DISA Dayton

Services	Ports	Prot	Designation	Policy		Conditions		Comments
				In	Out	In	Out	
Audit	5402	TCP	Yellow	Cond	Cond	- Allow inbound to only authorized servers	- Restrict by Destination IP	CAC Common Access Cards - USMC (added 30 March 2001)
WASP	5403	TCP	Yellow	Cond	Cond	- Allow inbound to only authorized servers	- Restrict by Destination IP	CAC Common Access Cards - USMC (added 30 March 2001)
WASP	5404	TCP	Yellow	Cond	Cond	- Allow inbound to only authorized servers	- Restrict by Destination IP	CAC Common Access Cards - USMC (added 30 March 2001)
DPAS	5557	TCP	Yellow	Cond	Cond	- Allow inbound to only authorized servers	- Restrict by Destination IP	* DISA Dayton
DPAS	5559	TCP	Yellow	Cond	Cond	- Allow inbound to only authorized servers	- Restrict by Destination IP	* DISA Dayton
Calendar	**5730**	**TCP**	**Red**	**Deny**	**Deny**			
WinVNC	5800	**UDP**	**Red**	**Deny**	**Deny**			
WinVNC	5900	**TCP**	**Red**	**Deny**	**Deny**			
X11	6000-6063	TCP/ UDP	Yellow	Cond	Cond	Restrict by source IP Restrict by destination IP	Restrict by source IP Restrict by destination IP	Recommend this service run through a VPN instead of open.
MS CHAT	**6665**	**TCP**	**Red**	**Deny**	**Deny**			
IRC	**6665-6669**	**TCP**	**Red**	**Deny**	**Deny**			
IRC	**6667**	**TCP**	**Red**	**Deny**	**Deny**			**See CERT/CC Advisory 94-14 and DOD CERT Bulletin 94-33.**
Subseven	**6711-6712**	**TCP**	**Red**	**Deny**	**Deny**			
Subseven	**6776**	**TCP**	**Red**	**Deny**	**Deny**			
MS CHAT listen	**7000**	**TCP**	**Red**	**Deny**	**Deny**			
Also subseven21								
DPAS	7001	TCP	Yellow	Cond	Cond	- Allow inbound to only authorized servers	- Restrict by Destination IP	* Navy Crane, DISA Huntsville
DPAS	7002	TCP	Yellow	Cond	Cond	- Allow inbound to only authorized servers	- Restrict by Destination IP	* NAVY Crane
DPAS	7003	TCP	Yellow	Cond	Cond	- Allow inbound to only authorized servers	- Restrict by Destination IP	* NAVY Crane
DPAS	7004	TCP	Yellow	Cond	Cond	- Allow inbound to only authorized servers	- Restrict by Destination IP	* NAVY Crane
DPAS	7005	TCP	Yellow	Cond	Cond	- Allow inbound to only authorized servers	- Restrict by Destination IP	* NAVY Crane
DPAS	7006	TCP	Yellow	Cond	Cond	- Allow inbound to only authorized servers	- Restrict by Destination IP	* NAVY Crane

Services	Ports	Prot	Designation	Policy		Conditions		Comments
				In	Out	In	Out	
DPAS	7007	TCP	Yellow	Cond	Cond	- Allow inbound to only authorized servers	- Restrict by Destination IP	* NAVY Crane, NAVY SEALIFT
V-ONE HTTP Encryption Tunnel	8000	TCP	Yellow	Cond	Cond	- Allow inbound to only authorized servers	- Restrict by Destination IP	* Pentagon
V-ONE HTTP Encryption Tunnel	8001	TCP	Yellow	Cond	Cond	- Allow inbound to only authorized servers	- Restrict by Destination IP	* Pentagon
HTTP-alt	8008	TCP	Green	Deny	Cond	- - Deny	- Relay Place http servers in DMZ	require the use of application layer proxying to more effectively control the use of this protocol.
HTTP-alt	8080	TCP	Green	Deny	Cond	- - Deny	- Relay Place http servers in DMZ	require the use of application layer proxying to more effectively control the use of this protocol.
Old SWA Ports	8999	TCP	Yellow	Cond	Cond	- Allow inbound to only authorized servers	- Restrict by Destination IP	* USMC
ASREQ Secure web server	9000	TCP	Yellow	Cond	Cond	- Allow inbound to only authorized servers	- Restrict by Destination IP	* DISA Columbus, DISA Huntsville, DISA Denver, DLA Richmond, NAVY SEALIFT
CS Listener (Oracle) / Knowledge Manager	9000	TCP	Yellow	Cond	Cond	- Allow inbound to only authorized servers	- Restrict by Destination IP	- identified as core basis for SID by DFAS ASREQ Secure web server Uses J-Initiator which must be downloaded out of band or through secure channel (see Mobil Code Policy)
SWA	9023	TCP	Yellow	Cond	Cond	- Allow inbound to only authorized servers	- Restrict by Destination IP	USMC (added 30 March 2001)
SWA	9024	TCP	Yellow	Cond	Cond	- Allow inbound to only authorized servers	- Restrict by Destination IP	USMC (added 30 March 2001)
SWA	9025	TCP	Yellow	Cond	Cond	- Allow inbound to only authorized servers	- Restrict by Destination IP	
SWA	9026	TCP	Yellow	Cond	Cond	- Allow inbound to only authorized servers	- Restrict by Destination IP	
HP JetDirect Printing	9100	TCP	Yellow	Cond	Cond	- Allow inbound to only authorized servers	- Restrict by Destination IP	* to DFAS from DISA
SARA	10005	TCP	Yellow	Cond	Cond	- Allow inbound to only authorized servers	- Restrict by Destination IP	Marine: Squadron Assistant Risk Assessment
MFCS	10500	TCP	Yellow	Cond	Cond	- Allow inbound to only authorized servers	- Restrict by Destination IP	* DISA Mechanicsburg
MFCS	10550	TCP	Yellow	Cond	Cond	- Allow inbound to only authorized servers	- Restrict by Destination IP	* DISA Mechanicsburg
NetBus	12345-12346	TCP	Red	Deny	Deny	-		

Services	Ports	Prot	Designation	Policy		Conditions		Comments
				In	Out	In	Out	
Deca Imaging System	13169	TCP	Yellow	Cond	Cond	- Allow inbound to only authorized servers	- Restrict by Destination IP	* DECA FT Lee, DECA Vienna
Stacheldraht	16660	**TCP**	**Red**	**Deny**	**Deny**			
DMS X.500	17003	TCP	Yellow	Cond	Cond	- Allow inbound to only authorized servers	- Restrict by Destination IP	
IGS Application	17499	TCP	Yellow	Cond	Cond	- Allow inbound to only authorized servers	- Restrict by Destination IP	* DISA Huntsville
CMIS	20001	TCP	Yellow	Cond	Cond	- Allow inbound to only authorized servers	- Restrict by Destination IP	* DISA Columbus
Trinoo	27444	**UDP**	**Red**	**Deny**	**Deny**	-		
Trinoo	27665	**TCP**	**Red**	**Deny**	**Deny**	-		
Defense Travel Service	31017	**TCP**	**Green**	**Deny**	**Allow**	-		PKI certificate required for use. Sessions are encrypted. Defense Travel Service Phone (703) 607-1498
Trinoo	31335	UDP	Red	Deny	Deny	-		
Back Orifice	31337-31338	TCP; UDP	Red	Deny	Deny	-		
RPC Services	32700-32900	**TCP; UDP**	**Red**	**Deny**	**Deny**	-		
Trinity V3	33270	**TCP**	**Red**	**Deny**	**Deny**	-		
Trinity V3	39168	**TCP**	**Red**	**Deny**	**Deny**	-		
Reachout	43188	TCP	Yellow	Cond	Cond	- Allow inbound to only authorized servers	- Restrict by Destination IP	* ARMY FT Stewart, ARMY FT Bliss, DISA Huntsville
Stacheldraht	**65000**	**TCP**	**Red**	**Deny**	**Deny**			
Audio streaming	**1025-65536**	**UDP**	**Red**	**Deny**	**Deny**			
Video streaming	**1025-65536**	**UDP**	**Red**	**Deny**	**Deny**			
JCALS	2223	UDP	Yellow	Cond	Cond	- Allow inbound to only authorized servers	- Restrict by Source IP	JCALS is permitted through the firewall on an as-needed basis through the use of a NAVSEA proxy. Recommend use in VPN only.
NIS			**Red**	**Deny**	**Deny**			
TOPS			Yellow	Cond	Cond	- Allow inbound to only authorized servers	- DMZ - Transition	

APPENDIX A
EVALUATION PROCESS

This guidance was developed by a technical advisory working group composed of representatives from the Joint Staff, DISA, NSA, the services and various CINCs, commands and agencies. Subsequently, this guidance was vetted through a formal DoD-wide review process. The working group used a discussion consensus approach, pooling knowledge on known vulnerabilities and modes of operation of the listed PPS. There was no new laboratory testing of vulnerabilities or mitigation techniques for this category assignment process. However, many of the participants brought knowledge and experience with prior security testing in their organizations' laboratories. While the working group focused on the technical issues of risk, there was some discussion of active use of many of the PPS by specific applications or systems on the NIPRNET. Therefore, in some cases the fact that a PPS is known to be essential to the operation of one or more applications influenced the assignment to the Yellow category, with appropriate mitigation techniques.

General Evaluation Principals

The primary evaluation principle considered was security risk. Risk was considered to be the vulnerabilities inherent in the use of the protocol and the application or service that uses the protocol combined with the risk that an adversary would attempt to exploit the vulnerability. Since little can be done from a security engineering perspective to affect the threat to a protocol or service, the focus of the analysis was on the vulnerability. Vulnerabilities can arise from many factors including poor identification, authentication or encryption, a lack of auditing, excessive privileges, or incomplete programming. Selected services should have very few if any well-known vulnerabilities. It is also desirable that the application using the specific service or protocol be small enough to be audited for security vulnerabilities. The actual table of PPS technical guidance can be found at Section 0 of this document and at http://www.cert.smil.mil.

When evaluating the PPS list, the technical working group used a number of general principles for operations of vulnerable data communication. Those principles include the following.

1. Identification and Authentication

Strong identification and authentication (I&A) is a fundamental security service that should be part of any protocol or service that traverses a security domain. Strong I&A can be defined as a method for ensuring the user or system can be irrefutably enumerated and that there is are mechanisms in place to make it extremely difficult for any other person or system to imitate the presentation of the credentials required for the transaction. Strong I&A should avoid the use of clear text transactions or the use of reusable authentication tokens. The I&A can be acceptable provided it takes place in any layer in the OSI stack, however if the protocol or service is to be filtered at the network or transport layer, there should be a mechanism in place to verify the protocol.

2. Encryption

Strong encryption should be part of any network connection that takes place across an untrusted network. Since this discussion is directed at considering network traffic that crosses a security perimeter, it is reasonable to expect that all traffic should be encrypted. In some cases, like e-mail, it may be desirable to only have the option of encrypting the traffic if and when it is necessary, for example using PKI. However, any encryption that is used should meet the robustness requirements of Reference 1.2.

3. Least Privileges

The application that is listening for a specific port or protocol should use as few privileges as possible. By embracing this principle it makes it more difficult for an attacker to directly gain privileged access to a system by exploiting vulnerability in the service. It can also increase the intrusion detection window by forcing an intruder to go through more steps to gain full access to a system.

4. Auditing

When it is necessary to allow traffic to cross a security perimeter, it is very desirable to ensure there is some level of audit present on the system that is likely to be targeted for attack. This can help prevent brute force attacks from being successful since the attacks can be detected well before they can correctly guess the password or cryptographic key. Auditing can also be helpful in detecting successful or failed attacks in progress.

5. Identified Vulnerabilities

There should always be some consideration given to whether or not there are any existing vulnerabilities in the application that will be used to accept connection from outside the security perimeter. If an application has a history of programming mistakes on the part of the developer, one could conclude that there may be additional vulnerabilities in current or future releases, and it may be undesirable to allow connections from untrusted sources. Clearly, some effort could be made to verify the listening applications have been correctly patched, however if the location at which security policy is being enforced is such that it is not practical to verify the state of all internal applications, then it may not be appropriate to allow the traffic to traverse the domain boundary.

6. Software Security Functional Audit

In general, the larger an application is, the more likely it is to include some programming error that could affect the security of the application. The smaller a program is the more likely it can be verified to function correctly by either the developer or, in some cases, the open source community or NIAP certified evaluation facility. Some consideration should be given to the size of the application that is accepting connections from untrusted source when determining whether or not it is prudent to allow the service across the security perimeter.